Department of Homeland Security

Information Analysis and Infrastructure Protection

"Snort stream4 Heap Overflow Vulnerability"
Advisory 03-018

April 17, 2003

The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) is issuing this advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029).

Snort is available in open source and commercial versions from Sourcefire, a privately held company headquartered in Columbia, MD. Details are available from Sourcefire. This vulnerability affect Snort versions 1.8.x through 1.9.1 and version 2.0 Beta. Sourcefire has announced that Snort 2.0 resolves this issue.

Researchers at CORE Security Technologies have discovered a remotely exploitable heap overflow in the Snort "stream4" preprocessor module. This module allows Snort to reassemble TCP packet fragments for further analysis. The Snort stream4 preprocessor (spp_stream4) incorrectly calculates segment size parameters during stream re-assembly for certain sequence number ranges which can lead to an integer overflow that can be expanded to a heap overflow.

The Snort stream4 flaw may lead to a denial of service (DoS) attack or remote command execution on a host running Snort. This attack can be launched by crafting TCP stream packets and transmitting them over a network segment that is being monitored by a vulnerable Snort implementation. In its default configuration, certain versions of snort are vulnerable to this attack, as is the default configuration of the Snort IDS.

The DHS/IAIP strongly recommends that system administrators or security managers who employ Snort take this opportunity to review their security procedures and patch or upgrade software with known vulnerabilities.

For further information, see the Core Security Technologies Advisory located at http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10, and Sourcefire advisory at http://www.sourcefire.com/services/advisories/sa041503.html.

Additional information may be found at Common Vulnerabilities and Exposure (CVE) Project http://www.CVE.mitre.org, and at CERT/CC, http://www.cert.org/.

As always, computer users are advised to keep systems software current by checking their vendor's web sites frequently for new updates and to check for alerts put out by the DHS/IAIP, CERT/CC, and other cognizant organizations. The DHS/IAIP encourages recipients of this advisory to report computer intrusions to appropriate law enforcement authorities including the FBI, http://www.fbi.gov/contact/fo/fo.htm, and the Secret Service, http://www.secretservice.gov. Recipients may report incidents online to http://www.nipc.gov/incident/cirr.htm. The DHS/IAIP Watch and Warning Unit can be reached at (202) 323-3205, 1-888-585-9078 or nipc.watch@fbi.gov.